UNITED STATES PATENT AND TRADEMARK OFFICE

mN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,019	03/30/2004	Vincent J. Zimmer	42339-199894	2791

26694 7590 07/18/2007

VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20043-9998

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/812,019	**Applicant(s)** ZIMMER ET AL.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-11,13-17,19 and 22-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-11,13-17,19 and 22-25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 May 2007* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed May 8, 2007, have been fully considered.

2. Claims 5-11, 13-17, 19, and 22-25 are pending and have been examined. Claims 1-4, 12, 18, 20, and 21 have been cancelled.

Information Disclosure Statement

3. It is noted that no Information Disclosure Statement has been filed on this application.

Specification

4. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code **found, for example, on page 5**. See MPEP § 608.01.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 14-17 and 19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are not limited to tangible embodiments. In view of applicants' disclosure, specification page 12, paragraph 40, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., media) and intangible embodiments (e.g., signals). As such, the claim is not limited to statutory subject matter and is therefore non-statutory.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 5-11, 13-17, 19, and 22-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Proudler et al. (US Patent 6,988,250, hereinafter Proudler).

Regarding claim 5, Proudler teaches

- a method of attestation comprising: connecting a computer having firmware and a trusted platform module (TPM) coupled to said firmware to a network **(abstract)**;
- determining a current platform trust state for said computer, wherein said current platform trust state is based on a current state of said firmware; receiving a challenge from a challenger on said network, wherein said challenger holds an enrolled platform trust state for said computer; signing said current platform trust state with a private portion of an attestation identity key (AIK) **(col. 7, lines 50-67, col. 8, lines 1-50)**;
- providing said signed current platform trust state to said challenger; and accessing said network when said signed current platform trust state matches said enrolled platform trust state **(col. 9, lines 1-67)**.

Regarding claim 8, Proudler teaches

- a method of provisioning, comprising: detecting a new computer on a network; challenging said new computer; receiving a current platform trust state, signed with a private portion of an attestation identity key (AIK), from said new computer **(abstract, col. 6, lines 1-55)**;
- comparing said signed current platform trust state with an enrolled platform trust state, wherein said enrolled platform trust state is signed by a privacy certificate authority **(col. 7, lines 50-67, col. 8, lines 1-50)**; and
- allowing said new computer to access said network when said enrolled platform trust state and said signed current platform trust state match.

Regarding claim 10, Proudler teaches

- an apparatus, comprising: a processor; firmware, coupled to said processor; a trusted platform module (TPM), coupled to said firmware **(abstract)**;
- a plurality of platform configuration registers (PCR) coupled to said TPM, wherein said PCRs contain a first.platform state signed by a privacy certificate authority; and an attestation identity key (AIK), maintained by said TPM, wherein said AIK comprises a public and private key **(col. 7, lines 50-67, col. 8, lines 1-50)**;
- wherein said TPM is operative to calculate a platform state signed with said private portion of said AIK according to a platform state contained in said PCRs, and is operative to provide said calculated platform state to a

challenging network; and wherein a comparison of said first platform state and said calculated platform state being identical indicates that the apparatus has not been tampered with **(col. 9, lines 1-67)**.

Regarding claim 14, Proudler teaches

- a machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising: detecting a new computer on a network, said computer having firmware and a trusted platform module (TPM); challenging said new computer **(abstract, col. 6, lines 1-55)**;
- receiving a current platform trust state signed with a private portion of an attestation identity key (AIK) from said new computer **(abstract, col. 6, lines 1-55)**;
- comparing said signed current platform trust state with an enrolled platform trust state, wherein said enrolled platform trust state is signed by a privacy certificate authority **(col. 7, lines 50-67, col. 8, lines 1-50)**; and
- allowing said new computer to access said network when said enrolled platform trust state and said signed current platform trust state match **(col. 9, lines 1-67)**.

Regarding claim 16, Proudler teaches

- a machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising: determining a current platform trust state for a computer having firmware and a trusted platform module (TPM) coupled to said firmware, wherein said current platform trust state is based on a current state of said firmware and said computer is coupled to a network **(abstract, col. 6, lines 1-55)**;

- receiving a challenge from a challenger on said network, wherein said challenger holds an enrolled platform trust state for said computer; signing said current platform trust state with a private portion of an attestation identity key (AIK) **(col. 7, lines 50-67, col. 8, lines 1-50)**;
- providing said signed current platform trust state to said challenger; and accessing said network when said signed current platform trust state matches said enrolled platform trust state **(col. 9, lines 1-67)**.

Regarding claims 6 and 17, Proudler teaches wherein said TPM comprises a plurality of platform configure registers (PCR) and determining a current platform trust state comprises: performing a hash-extend operation on contents of said PCRs **(col. 7, lines 1-67, col. 9, lines 1-67)**.

Regarding claim 7, Proudler teaches provisioning said computer across said network **(col. 8, lines 1-50)**.

Regarding claim 9, Proudler teaches verifying trust in said privacy certificate authority; and allowing said new computer to access said network when said privacy certificate authority is trustworthy **(col. 8, lines 1-67)**.

Regarding claim 13, Proudler teaches wherein said firmware is operative to provide said public key of said AIK and said platform trust state without an operating system running on said processor **(col. 7, lines 14-67, col. 8, lines 1-25)**.

Regarding claim 15, Proudler teaches wherein the software code causes the computer to perform the method further comprising: verifying trust in said privacy certificate authority; preventing said new computer from accessing said network when said privacy certificate authority is not trustworthy; and allowing said new computer to access said network when said privacy certificate authority is trustworthy **(col. 7, lines 14-67, col. 8, lines 1-25)**.

Regarding claim 22, Proudler teaches prior to connecting said computer to said network: bundling an identification (ID) request for said computer; sending said ID request to a privacy certificate authority; receiving a verified and signed ID from said privacy certificate authority; and installing said verified and signed ID on said firmware **(col. 9, lines 1-67)**.

Regarding claims 11, 19, and 23, Proudler teaches wherein said firmware is at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS **(col. 6, lines 25-67)**.

Regarding claim 24, Proudler teaches wherein bundling an ID request comprises bundling at least one of a new public ID key, an endorsement certificate, a platform certificate, or a conformance certificate into said ID request **(col. 9, lines 1-67)**.

Regarding claim 25, Proudler teaches wherein said new public ID key is a public portion of an attestation identity key (AIK), said AIK having a public portion and a private portion, wherein said private portion is maintained by said TPM **(col. 6, lines 1-67, col. 9, lines 1-67)**.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

11. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7, 12, 07